United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with Snapchat Accounts "codyr819" and "agteachercody" that is Stored at a Premises Controlled by Snap, Inc.	**Case No. 25-MJ-128-DES**

APPLICATION FOR SEARCH WARRANT

I, Blair Newman, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **NORTHERN** District of **CALIFORNIA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2252(a)(2) & 2252A(a)(2) and the application is based on these facts:

☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Blair Newman, Special Agent
FBI

Sworn to :

Date: April 3, 2025

City and state: Muskogee, Oklahoma

Judge's signature

D. EDWARD SNOW
UNITED STATES MAGISTRATE JUDGE
Printed name and title

Affidavit in Support of
An Application for a Search Warrant

I, Blair Newman, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with the Snapchat user accounts "codyr819" and "agteachercody" (hereafter "**TARGET ACCOUNTS**") that is stored at premises owned, maintained, controlled, or operated by Snap, Inc. ("Snap" or "Snapchat"), headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A), to require Snap Inc. to disclose to the government Snapchat records and other information in its possession, including the contents of communications, as further described in Attachment B, pertaining to the subscriber or customer associated with the **TARGET ACCOUNTS.**

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2019. I am assigned to the Tulsa Resident Agency of the Oklahoma City Division. My primary duties as a Special Agent with the FBI include but are not limited to investigating crimes against children.

3. Specifically, I have extensive experience working cases involving child pornography and child exploitation in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. All these cases have

required the review of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As such, I am familiar with the tactics utilized by individuals who collect, distribute, and or produce child pornographic material.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe the **TARGET ACCOUNTS** described in Attachment A contain evidence of violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (Receipt of Child Pornography) by **Cody Ryan Richison.**

Jurisdiction

6. "[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

> a. Title 18, United States Code, Section 2252(a)(2) makes it a federal crime if any person knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate of foreign commerce or through the mails, if the producing of

such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the facts and circumstances alleged in this affidavit occurred within the Eastern District of Oklahoma.

Definitions

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. "Child erotica" is materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or electronic device to access the Internet. IP addresses can be dynamic, meaning that the ISP

assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

f. "Cloud storage service" refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit.

g. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

h. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

i. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

j. "Chat" refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

k. "Chat room" is the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

l. "Mobile applications" are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

Snapchat Background

10. Based on my training and experience, information acquired from other law enforcement officials with technical expertise, and the Snapchat Law Enforcement Guide, I know the following information concerning Snapchat:

a. Snapchat is a product offered by Snap, Inc. ("Snap"), a company headquartered in Venice, California. Snapchat is a free access social networking application (or "app") that can be accessed at http://www.snapchat.com. Snapchat is an application for sending and receiving "self-destructing" messages, pictures, and videos. These messages are commonly referred to as "snaps."

b. A "snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long their snap can be viewed. Once a snap has been viewed it is deleted from Snap's system and is no longer visible to the recipient.

c. Snapchat users can also send text messages to others using Snapchat's "Chat" feature. Once a user leaves the Chat screen within the application, messages viewed by both the sender and the receiver will exist for only a predetermined amount of time. Then the Snap system deletes the messages. Snapchat further notifies other users when a user is online, and users can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from an archive of saved pictures in the photo gallery of the device. Snapchat users compile contact lists of other users, with whom they can communicate. In light of the foregoing, Snapchat constitutes a provider of an "electronic communication service" within the meaning of 18 U.S.C. § 3123. See 18 U.S.C. §§ 3127(1) and 2510(15).

d. A Snapchat username is a unique identifier associated with a specific account on Snapchat and cannot be changed by the user. On the other hand, a Snapchat vanity name is not a unique identifier and can be set and changed by a user or that user's friends to indicate how the user will appear within the app. Unlike a username, a vanity name can contain special characters and symbols beyond hyphen, underscore, or period, as well as spaces, emojis, and capital letters.

e. "Our Story" is a collection of the user's submitted "snaps" from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a concert could all contribute to the same "Our Story" collection by sharing their snaps, even if they do not know each other. Users can also view "Our Story" events if they are not actually present at the event by subscribing to the story.

f. A Snapchat user can keep a public photo/video diary using the "My Story" feature. Each snap in a user's "My Story" documents the user's experience. Based on the user's privacy settings, the photos and videos added to "My Story" can be viewed either by everyone on Snapchat or just the user's friends. Stories are visible to other users for up to 24 hours.

g. Snapchat has a "Group Stories" feature allowing multiple users to contribute photos and videos to the same "Story", a collection of posts that stay viewable for a limited amount of time. Snapchat users have the ability to name their group story and invite other users by username to add content to the group story. The group stories will disappear if 24 hours pass without a user adding a new photo or video.

h. Snapchat "Memories" is a cloud-storage service hosted by Snapchat. Snapchat users can save their sent or unsent snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. A user can also edit and send snaps and create Stories from these Memories. Snaps, Stories, and other photos and videos saved in Memories are backed up by Snapchat and may remain in Memories until deleted by the user.

i. While a Snapchat message or "snap" may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap or message. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

j. Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account, they make a unique Snapchat username. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account and a new user is prompted to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code which must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

k. Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

l. In some cases, users of social networking applications will communicate directly with the application about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Application providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications. In addition, application providers often have records of the IP addresses used to register the account and

the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access the account and their geographic location.

m. Data maintained on computer servers maintained, used or owned by Snap, Inc. can contain stored information for the **TARGET ACCOUNTS** to include:

n. Stored electronic content as well as connection log files listing account activity done by the subscriber/user associated with the above-described Snapchat user account, including dates, times, methods of connecting to the Internet and accessing Snapchat.

o. Saved chat logs, previous Snaps, Snapchat stories and Snapchat chats sent to or from the **TARGET ACCOUNTS**.

p. Snapchat "Groups" for which the **TARGET ACCOUNTS** are a member or otherwise associated.

q. Information stored in connection with a Snapchat account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Snapchat user's account activity, IP log, stored electronic communications, and other data retained by Snapchat, can indicate who has used or controlled the Snapchat account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, Snapchat chat logs, shared photos and videos, and captions (and the data associated with the foregoing, such

as geo-location, date and time) may be evidence of who used or controlled the Snapchat account at a relevant time. Further, Snapchat account activity can show how and when the account was accessed or used.

r. In my training and experience, evidence of who was using an application account may be found in address books, contact or buddy lists, telephone numbers, email addresses in the account, and attachments to electronic messages, including pictures and files.

Probable Cause

11. 10. On August 7, 2024, FBI Agents interviewed Joseph Gunther Sampson, who confessed to viewing, receiving, and sending child pornography. Sampson provided Agents with consent to search multiple electronic devices, to include his iPhone SE. On September 16, 2024, Sampson was indicted in the Northern District of Oklahoma (24-CR-298) and charged with Receipt and Distribution of Child Pornography and Possession of Child Pornography in Indian Country.

12. In November 2024, I reviewed an extraction of Sampson's iPhone SE and identified text messages sent between Sampson and telephone number 405-564-2463, which law enforcement databases and open source research identified as belonging to Cody Ryan Richison, date of birth XX/XX/1990, and home address XXXX N 375 Road, Holdenville, Oklahoma 74848. Research further revealed Richison was an Agricultural Education Instructor at Holdenville High School and a Future Farmers of America (FFA) Advisor. The text messages were exchanged on January 26, 2024, and included the following:

Sampson: You really want to do the pedo[1] family thing?
Richison: Yes I do. Do you?
Sampson: God yes
…

[1] I know from my training and experience that that the term "pedo" is a slang reference for "pedophilia."

Sampson: You fucked an underage?
…
Sampson: Whats youngest youve been in?
…
Richison: 10

Sampson: Hmmm fuck yes
Richison: A buddy's foster son.

Richison: There's a guy in henryetta that has a 3-4 yo
Sampson: 😊
Richison: He's on Tele

13. Richison was also the subject of National Center for Missing and Exploited Children (NCMEC) CyberTipline Report 197677580. According to the report, S.E. called to report his ex-partner, J.L., confessed to him in April 2024 that he was cheating on him with Richison. J.L. also disclosed to S.E. that Richison was in possession of child pornography on his cell phone. J.L. stated that one day Richison left his phone unlocked and he observed child pornography on it.

14. On December 4, 2024, Agents executed three sealed, federal search warrants for the person of CODY RYAN RICHISON, a premises at XXXX N 375 Road, Holdenville, Oklahoma 74848, and the white Ford F-150 truck with VIN 1FTPW14V19FA70397, respectively 24-MJ-394-DES, 24-MJ-393-DES, and 24-MJ-392-DES. During the execution of the search warrants, Agents located RICHISON, who agreed to speak with Agents. During a post-Miranda interview, RICHISON made numerous incriminating statements, including but not limited to:

- RICHISON received approximately 100 photos and videos of children being sexually abused from C.S.[2], beginning in approximately 2020. The children being sexually abused were both male and female, and their ages ranged, but included children as young as

[2] C.S. is an individual known to law enforcement and is currently the subject of a prosecution for child sexual exploitation.

infants. RICHISON received at least one of these images in March 2024 while he was employed as a teacher at Holdenville High School in the Eastern District of Oklahoma. RICHISON knew his actions were wrong.

- RICHISON worked with children every day. RICHISON recently talked with a friend about becoming a foster parent.
- RICHISON knew what happened to "CHOMOS"[3] in prison because he previously worked in a correctional facility.

15. During the execution of the search warrants, Agents seized Richison's iPhone 14 Pro Max S/N DK2K02K071, hereinafter "Richison's iPhone," pursuant to 24-MJ-394-DES.

16. On December 10, 2024, the Honorable Gerald L. Jackson, United States Magistrate Judge, Eastern District of Oklahoma, signed 24-MJ-405-GLJ, authorizing the search of Richison's iPhone. On December 4, 2024, when Richison's iPhone was seized from Richison, Agents placed Richison's iPhone in Airplane Mode, per best practice.

17. On December 12, 2024, FBI personnel attempted to extract Richison's iPhone pursuant to 24-MJ-405-GLJ. Previously unbeknownst to the Agents, when Richison's iPhone was placed into Airplane Mode, Stolen Device Protection feature was activated, potentially due to Richison's user settings.

18. Upon plugging Richison's iPhone into an FBI-authorized tool, FBI personnel selected "trust" on Richison's iPhone to begin the extraction. At that time, Richison's iPhone prompted FBI personnel for Face ID with a message containing the header, "Face ID required" and the text, "Stolen Device Protection is turned on." As a result, FBI personnel were unable to extract Richison's iPhone.

[3] I know from my training and experience that the term "chomos" is a slang reference for "child molesters."

19. On December 12, 2024, the Honorable Gerald L. Jackson, United States Magistrate Judge, Eastern District of Oklahoma, signed 24-MJ-414-GLJ, authorizing the search of Richison's iPhone with biometric access.

20. On December 17, 2024, pursuant to 24-MJ-414-GLJ, the FBI utilized Richison's Face ID and subsequently extracted Richison's iPhone.

21. Between December 17, 2024 and February 21, 2025, the FBI reviewed the extraction of Richison's iPhone and identified the **TARGET ACCOUNTS**. There were also multiple videos on Richison's iPhone, received via Snapchat, depicting "age difficult" pornographic material.

22. The FBI requested Snap, Inc. preserve the **TARGET ACCOUNTS** on November 14, 2024, and extended the preservation request on February 11, 2025. Snap, Inc. confirmed the accounts would be preserved through May 3, 2025. The reference number for the request is 259983986.

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children and Individuals who Distribute, Receive, Possess and/or Access with Intent to View Child Pornography

23. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings

or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is

abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted"[4] it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

j. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Background on Child Pornography, Computers, and the Internet

24. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, smartphones[5] and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file

[5] Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Information to be Searched and Things to be Seized

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B, as they pertain to

the **TARGET ACCOUNTS** described in Attachment A. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

40. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. I therefore request authority for the warrant to be executed at any time of the day or night.

Conclusion

41. Based on the information set forth in this affidavit, I respectfully submit that there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (Receipt of Child Pornography) as further described in Attachment B, are likely to be located in the **TARGET ACCOUNTS** described in Attachment A, and I request that the Court issue the proposed search and seizure warrant.

42. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Blair Newman, Special Agent
FBI

Sworn to on April 3rd, 2025.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the Snapchat accounts "codyr819" and "agteachercody" (hereafter "**TARGET ACCOUNTS**") which is stored at the premises owned, maintained, controlled, or operated by Snap, Inc., ("Snapchat") which is headquartered at 2772 Donald Douglas Loop North, Santa Monica, California 90405.

ATTACHMENT B

Particular Things to be Seized

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, Inc, including any Snapchat messages, Snaps, records, files, logs, or information that have been deleted but are still available to Snapchat, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snapchat is required to disclose the following information to the government for each account listed in Attachment A:

(a) All identity and contact information, including full name, email address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;

(b) All past and current usernames associated with the account;

(c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(d) All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;

(e) All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

(f) All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

(g) The contents of all communications or other messages sent or received by or stored in the account, including stored or preserved copies of Snaps, Stories, Memories,

Chats, and other messages sent to and from the account; drafts; the source and destination accounts associated with each message; and the date and time at which each message was sent or received from January 1, 2019, to present;

(h) All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content from January 1, 2019, to present;

(i) All photographs and images in the user gallery for the account from January 1, 2019, to present;

(j) All location data associated with the account, including geotags;

(k) All data and information that has been deleted by the user;

(l) A list of all users that the account has "unfollowed" or blocked;

(m) All privacy and account settings;

(n) All records of Snapchat searches performed by the account, including all past searches saved by the account;

(o) All information about connections between the account and third-party websites and applications; and,

(p) All records pertaining to communications between Snapchat and any person regarding the user or the user's Snapchat account, including contacts with support services, and all records of actions taken, including suspensions of the account.

I. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (Receipt of Child Pornography) along with any attempts or conspiracy to engage in such conduct,

including for the **TARGET ACCOUNTS** listed in Attachment A, information pertaining to the following matters:

A. Production or attempted production of child pornography;

B. The possession and access with intent to view child pornography images or material involving the sexual exploitation of minors, constituting violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2);

C. The receipt and/or distribution of child pornography, constituting violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2);

D. Records and communications tending to show or evidence a sexual interest in minors, including a desire or motive to receive, distribute, or present visual depictions of minors engaged in sexually explicit conduct;

E. Evidence indicating how and when the Snapchat account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

F. Evidence indicating the Snapchat account owner's state of mind as it relates to the crime under investigation;

G. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and

H. The identity of the person(s) who communicated with the user ID about matters relating to violations of 18 U.S.C. § 2251(a) and (e) (production or attempted production of child pornography), 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct), including records that help reveal their whereabouts

and records and information tending to show a conspiracy to receive, distribute, possess, or access visual depictions of minors engaged in sexually explicit conduct.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.